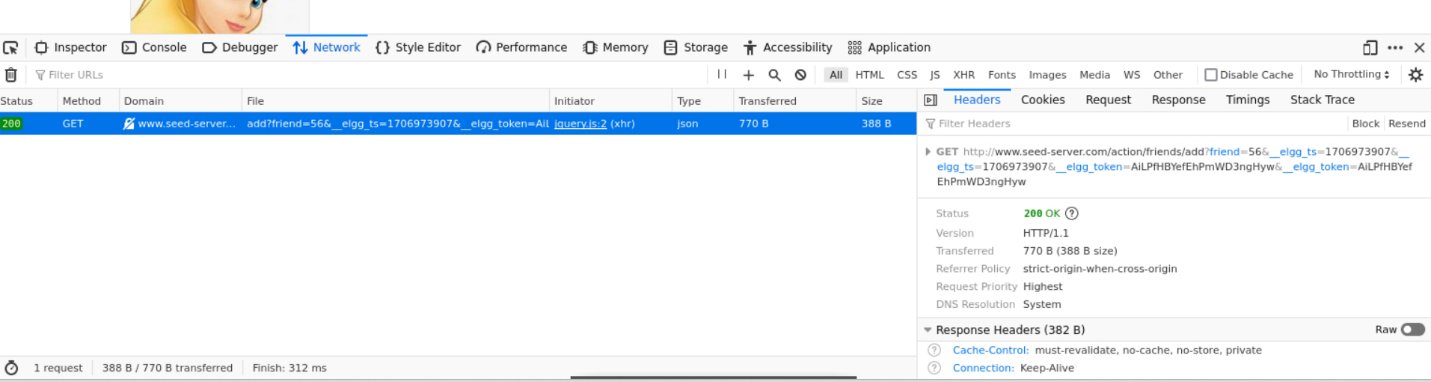
**Report on Offline 2 on XSS**

**CSE 406 – Computer Security Sessional**

**Roll : 1905014**

**Task -1:**

To become the victim’s friend, the url for adding a friend was to be determined. I did this by examinig the GET request that is sent when a user adds someone as a friend.

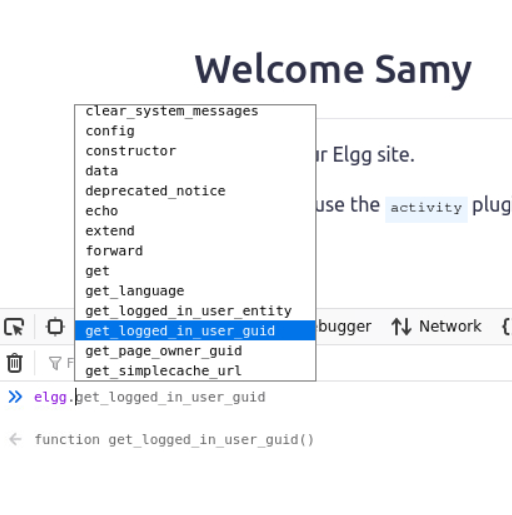


I had to determine the id number of Samy’s profile. When the “View Page Source” of Samy’s starting page is clicked, the guid and other information is found at the bottom of the page:



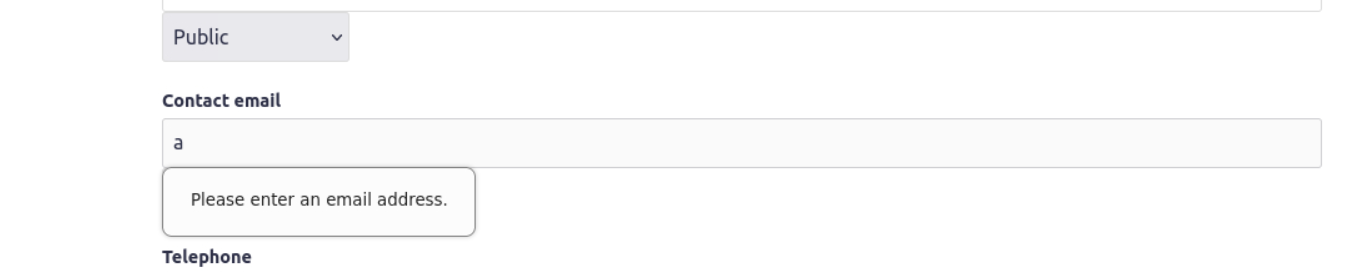
There are also the elgg functions found through Console tab of “Inspect” which are used to determine the current (logged in) user’s name, username, guid, profile url etc.

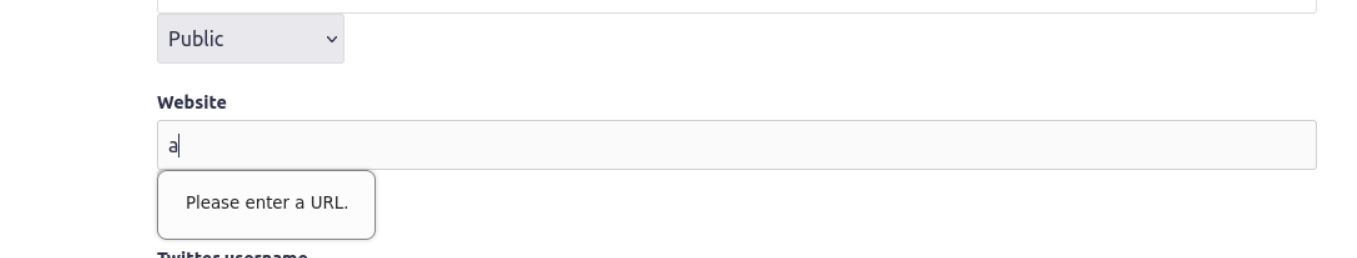




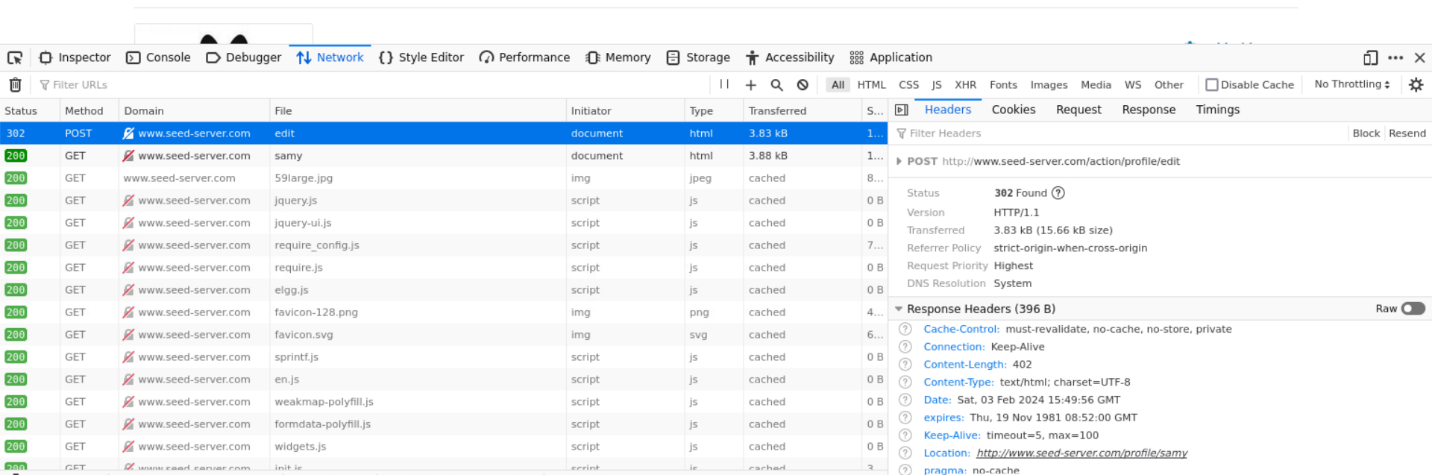
**Task – 2:**

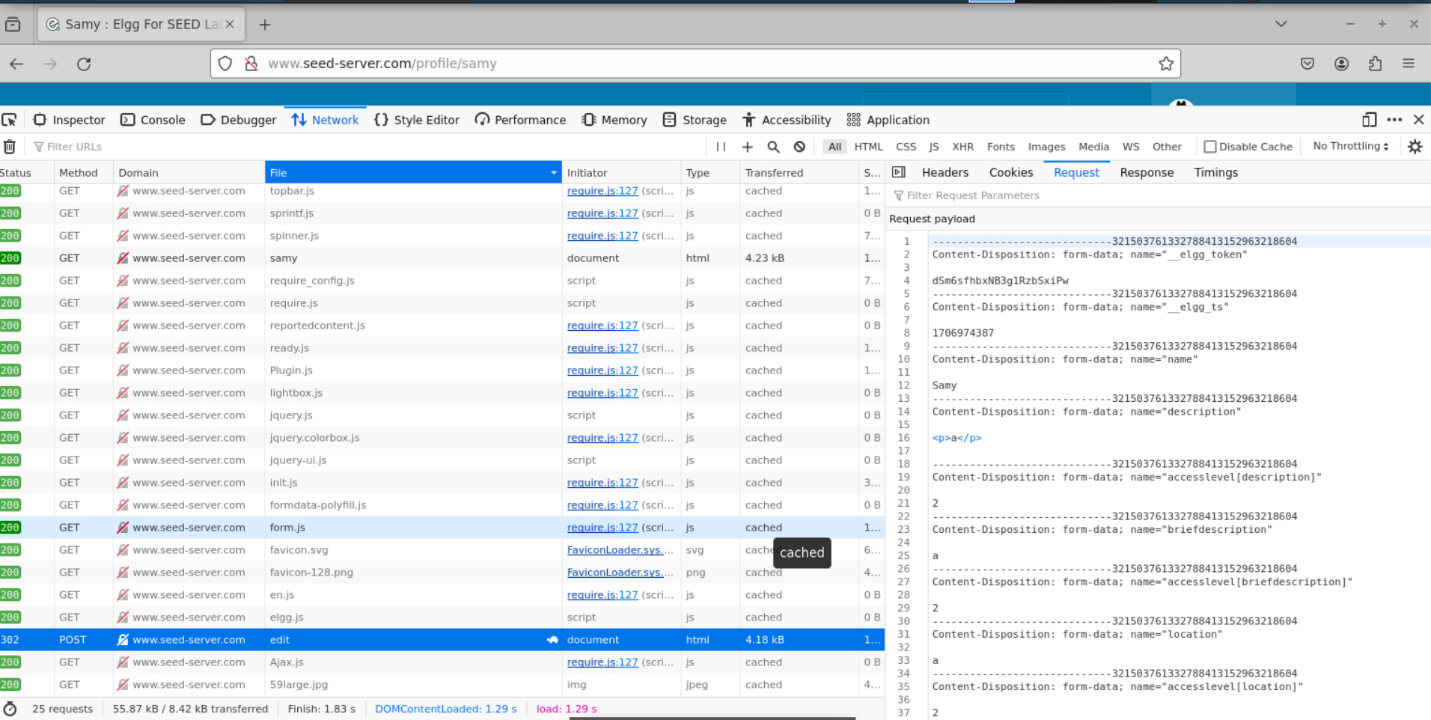
For task 2, at first the input format of the fields are determined by adding random input to the fields in Samy’s profile:



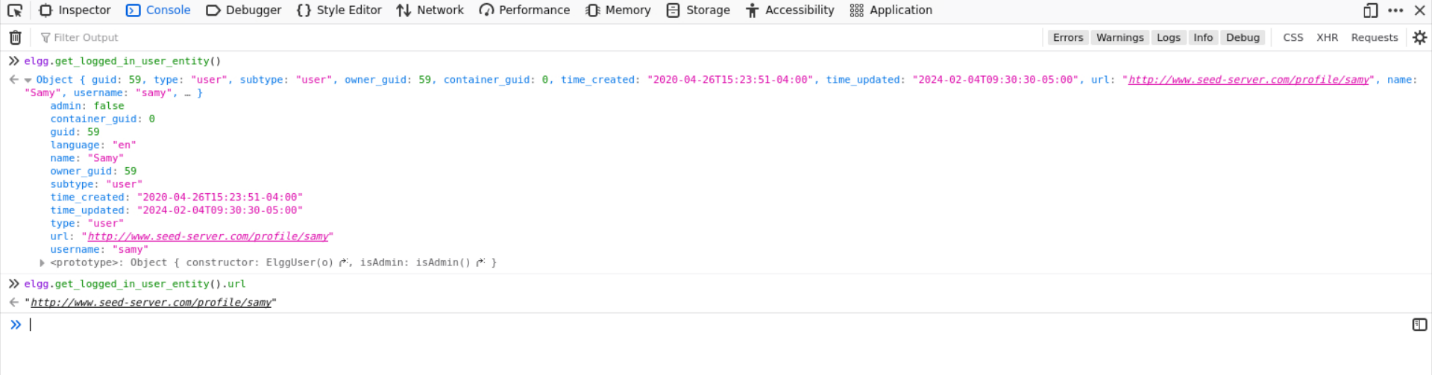


The url for editing profile, request body of the change along with access code and the user’s name were found by simply examining the POST request in the Network tab of “Inspect”.



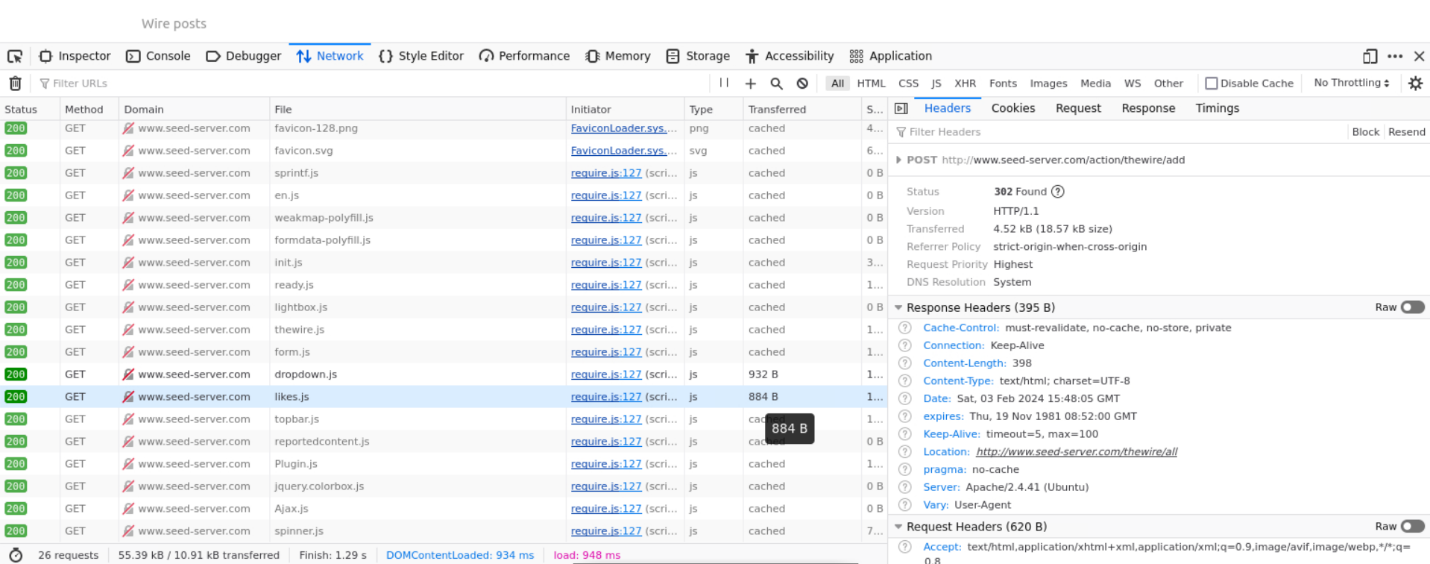


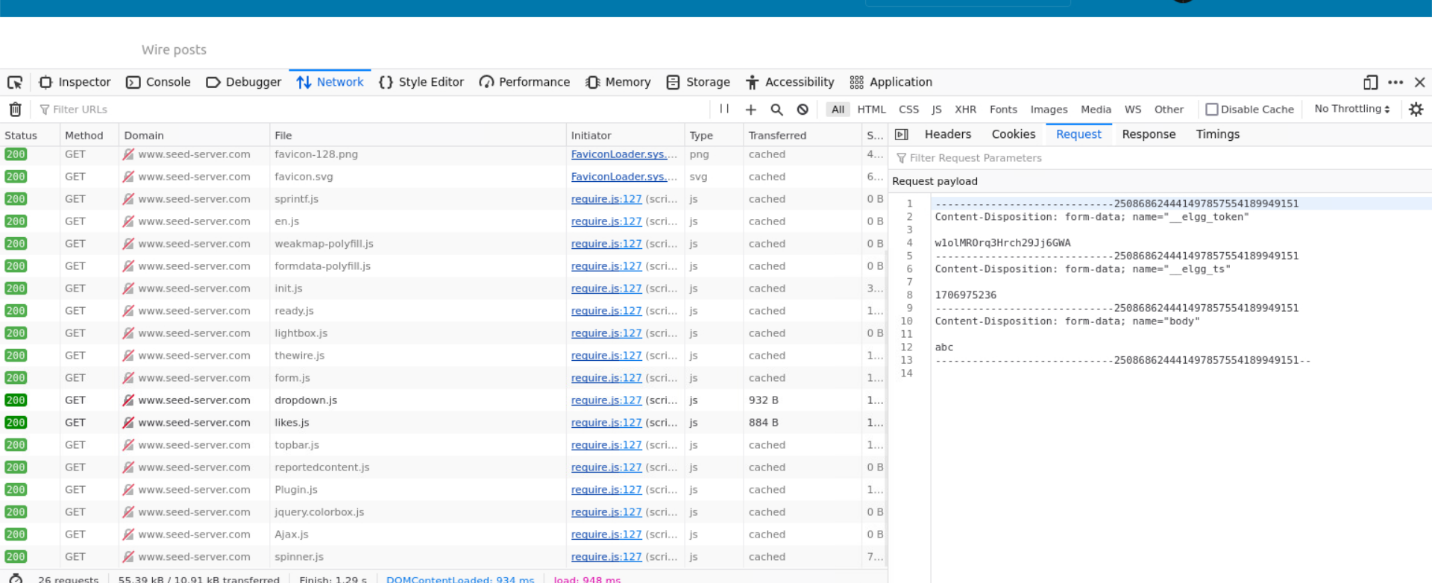
The user’s name was determined by the elgg function to obtain logged in user’s entity.



**Task – 3:**

Here, the url for posting on the wire and its request body was to be determined. This was done by again examining the POST request in the Network tab of “Inspect”.





**Task – 4:**

Task 4 is a combination of all the previous tasks. Here, the wormcode needs to be propagated with DOM API, whose code was already provided. The difference is that instead of Samy’s profile for task 3, the infected user had to link their own profile in The Wire post. The url of a person’s profile is determined through the elgg function to get the user’s entity and url.

